UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AARON GOLLAND; TIMOTHY PARKER; JOSE SANTIAGO; and LANCE SMITH, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

MAJOR LEAGUE BASEBALL ADVANCED MEDIA, L.P.,

Defendant.

Case No. 1:24-cv-6270

FIRST AMENDED CLASS ACTION COMPLAINT & DEMAND FOR JURY TRIAL

Plaintiff **AARON GOLLAND** ("Plaintiff Golland"), Plaintiff **TIMOTHY PARKER** ("Plaintiff Parker"), Plaintiff **JOSE SANTIAGO** ("Plaintiff Santiago"), and Plaintiff **LANCE SMITH** ("Plaintiff Smith") (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, make the following allegations pursuant to the investigation of counsel and based upon information and belief, except as to allegations pertaining specifically to themselves or their counsel, which are based on personal knowledge.

NATURE OF THE CASE

1. Plaintiffs bring this action for legal and equitable remedies to redress and end Defendant **MAJOR LEAGUE BASEBALL ADVANCED MEDIA L.P.**'s practices of knowingly selling, transmitting, and/or otherwise disclosing, to Meta Platforms, Inc. ("Meta") and various third parties, records containing the personal information (including names and addresses) of each of its website and streaming service subscribers, along with detailed information revealing the titles and subject matter of the videos and other audiovisual materials requested or obtained by each of its subscribers (collectively "Personal Viewing Information") in violation of the Video Privacy Protection Act, 18 U.S.C. §2710, et seq. ("VPPA").

2. Defendant operates the subscription-based website MLB.com. MLB.com hosts affiliate websites for each of the thirty Major League Baseball teams, accessible at MLB.com/[team name], all of which contain prerecorded video content. Defendant operates a subscription-based streaming service accessible at MLB.tv which also contains prerecorded video content.[1]

3. Over the past two years, Defendant has systematically transmitted (and continues to transmit today) its website and streaming service subscribers' personally identifying video viewing information to third parties such as Meta and Snap Inc. ("Snapchat") via tracking pixel technologies. The pixel developed by Meta and employed by Defendant for the purpose of making these transmissions is called the "Meta Pixel." The pixel developed by Snapchat and employed by Defendant for the purpose of making these transmissions is called the "Snapchat Pixel." Defendant knowingly and intentionally installed the Meta Pixel and Snapchat Pixel on its MLB.com Website and its MLB.tv streaming service.[2]

4. The information Defendant disclosed (and continues to disclose) to Meta, via the Meta Pixel it installed on its website, includes the website or streaming service subscribers' Facebook ID ("FID") coupled with the title of each of the specific videos that the subscriber requested or obtained on Defendant's website. A subscriber's FID is a unique sequence of numbers linked to the Meta profile belonging to that subscriber. The subscriber's Meta profile, in turn,

[1] The word "website" as used herein refers collectively to MLB.com and its hosted team websites.

[2] The MLB.com Website is the platform that delivers all prerecorded video content. Defendant uses the moniker, MLB.tv for its streaming service, which requires a separate purchase and subscription available on a sub-domain, commerce.mlb.com. Because the subscription to the base website is different from the subscription to the streaming service, this complaint refers to content exclusively available through Defendant's streaming service as being provided by "MLB.tv" or "Defendant's streaming service" interchangeably.

publicly identifies the subscriber by name (and contains other personally identifying information about the subscriber as well). Entering "facebook.com/[FID]" into a web browser returns the Meta profile of the person to whom the FID corresponds. Thus, the FID identifies a person more precisely than a name, as numerous persons may share the same name but each person's Facebook profile (and associated FID) uniquely identifies one and only one person. In the simplest terms, the Meta Pixel installed by Defendant captures and discloses to Meta information that reveals that a subscriber purchased a subscription to access prerecorded videos via Defendant's streaming service and the specific videos that a particular person viewed as a subscriber of Defendant's website.

5. The information Defendant disclosed (and continues to disclose) to Snapchat via the Snapchat Pixel includes the consumer's email address, the purchase of a streaming service subscription, and the particular videos that a subscriber requested or obtained while on the website or streaming service. A cellular telephone number or email is required to sign up for a Snapchat account. A Snapchat profile, in turn, publicly identifies by name the specific person to whom the profile belongs (and also contains other personally identifying information about the person). Entering the cellular telephone number on any search engine or a free reverse lookup site will return the owner's name. Thus, the cellular telephone number used for sign-up identifies a person more precisely than a name, as numerous persons may share the same name, but a cellular telephone number is usually uniquely associated with one and only one person. In the simplest terms, the Snapchat Pixel installed by Defendant captures and discloses to Snapchat information that a subscriber purchased a subscription to access prerecorded videos via Defendant's streaming service and the specific videos that a particular person viewed as a subscriber to Defendant's website or streaming service.

6. Defendant disclosed and continues to disclose its subscribers' Personal Viewing Information to Meta and Snapchat without asking for, let alone obtaining, its subscribers' consent to these practices.

7. The VPPA clearly prohibits what Defendant has done. Subsection (b)(1) of the VPPA provides that, absent the consumer's prior informed, written consent, any "video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for," 18 U.S.C. § 2710(b)(1), inter alia, liquidated damages in the amount of $2,500.00 per violation and equitable relief, *see id.* § 2710(c).

8. Accordingly, on behalf of themselves and the members of the putative classes defined below, Plaintiffs bring this First Amended Class Action Complaint against Defendant for intentionally and unlawfully disclosing their Personal Viewing Information to third parties.

PARTIES

I. Plaintiff Golland

9. Plaintiff Golland is, and at all times relevant hereto was, a citizen and resident of West Nyack, New York.

10. Plaintiff Golland is, and at all times relevant hereto was, a user of Meta.

11. Plaintiff Golland is a consumer of the video products and services offered on Defendant's MLB.tv streaming service. He first subscribed to Defendant's streaming service in or about March 2024, and has continuously maintained his subscription since then. Plaintiff Golland became a subscriber to Defendant's streaming service by registering and paying for a subscription via Defendant's website, including by providing his name, email address, payment information, and zip code.

12. On multiple occasions during the two years preceding the filing of this action, Plaintiff Golland used his subscription to Defendant's streaming service to request and obtain prerecorded videos from Defendant. On each such occasion, Defendant disclosed to Meta Plaintiff Golland's FID coupled with the specific title of the video he requested and obtained and the URL where he requested access to and obtained the video, among other information concerning Plaintiff Golland and the device on which he used to request and obtain the video.

13. At all times relevant hereto, including when purchasing prerecorded video material from Defendant's streaming service, Plaintiff Golland had a Meta account, a Meta profile, and an FID associated with such profile.

14. Plaintiff Golland has never consented, agreed, authorized, or otherwise permitted Defendant to disclose his Personal Viewing Information to Meta. In fact, Defendant has never even provided Plaintiff Golland with written notice of its practices of disclosing its subscribers' Personal Viewing Information to third parties such as Meta.

15. Because Defendant disclosed Plaintiff Golland's Personal Viewing Information (including his FID, the title of the prerecorded video material he requested or obtained from Defendant's streaming service as a paying subscriber, and the URL where such video is available to paying subscribers) to Meta during the applicable statutory period, Defendant violated Plaintiff Golland's rights under the VPPA and invaded his statutorily conferred interest in keeping such information (which bears on his personal affairs and concerns) private.

II. Plaintiff Parker

16. Plaintiff Parker is, and at all times relevant hereto was, a citizen and resident of Bardstown, Kentucky.

17. Plaintiff Parker is, and at all times relevant hereto was, a user of Meta.

18. Plaintiff Parker is a consumer of the video products and services offered on Defendant's MLB.tv streaming service. He first subscribed to Defendant's streaming service in or about March 2024, and has continuously maintained his subscription since then. Plaintiff Parker became a subscriber to Defendant's streaming service by registering and paying for a subscription via the mobile version of Defendant's website, including by providing his name, email address, payment information, and zip code.

19. On multiple occasions during the two years preceding the filing of this action, Plaintiff Parker used his subscription to Defendant's streaming service to request and obtain prerecorded videos from Defendant. On each such occasion, Defendant disclosed to Meta Plaintiff Parker's FID coupled with the specific title of the video he requested and obtained and the URL where he requested access to and obtained the video, among other information concerning Plaintiff Parker and the device on which he used to request and obtain the video.

20. At all times relevant hereto, including when purchasing prerecorded video material from Defendant's streaming service, Plaintiff Parker had a Meta account, a Meta profile, and an FID associated with such profile.

21. Plaintiff Parker has never consented, agreed, authorized, or otherwise permitted Defendant to disclose his Personal Viewing Information to Meta. In fact, Defendant has never even provided Plaintiff Parker with written notice of its practices of disclosing its subscribers' Personal Viewing Information to third parties such as Meta.

22. Because Defendant disclosed Plaintiff Parker's Personal Viewing Information (including his FID, the title of the prerecorded video material he requested or obtained from Defendant's website as a paying subscriber, and the URL where such video is available to paying subscribers) to Meta during the applicable statutory period, Defendant violated Plaintiff Parker's

rights under the VPPA and invaded his statutorily conferred interest in keeping such information (which bears on his personal affairs and concerns) private.

III. Plaintiff Santiago

23. Plaintiff Santiago is, and at all times relevant hereto was, a citizen and resident of Akron, Ohio.

24. Plaintiff Santiago is, and at all times relevant hereto was, a user of Meta and Snapchat.

25. Plaintiff Santiago is a consumer of the video products and services offered on Defendant's MLB.tv streaming service. He first subscribed to Defendant's streaming service in or about March 2023, and has continuously maintained his subscription since then. Plaintiff Santiago became a subscriber to Defendant's streaming service by registering and paying for a subscription via his Apple TV account, including by providing his name, email address, payment information, and zip code.

26. At all times relevant hereto, including when requesting or obtaining prerecorded video material from Defendant on its website, Plaintiff Santiago had a Meta account, a Meta profile, and an FID associated with such profile.

27. At all times relevant hereto, including when purchasing a subscription to Defendant's streaming service and accessing and obtaining the prerecorded video material provided to subscribers, Plaintiff Santiago had a Snapchat account, a Snapchat profile, and his cellular telephone number was associated with such profile.

28. On each such occasion, Defendant disclosed to Meta Plaintiff Santiago's FID coupled with the specific title of the video he requested and obtained and the URL where he requested access to and obtained the video, among other information concerning Plaintiff Santiago

and the device on which he used to request and obtain the video. Also, on each such occasion, Defendant disclosed to Snapchat Plaintiff Santiago's persistent account identifier and email address coupled with the specific title of the video he requested and obtained and the URL where he requested access to and obtained the video, among other information concerning Plaintiff Santiago and the device on which he used to request and obtain the video.

29. Plaintiff Santiago has never consented, agreed, authorized, or otherwise permitted Defendant to disclose his Personal Viewing Information to Meta or Snapchat. In fact, Defendant has never even provided Plaintiff Santiago with written notice of its practices of disclosing its subscribers' Personal Viewing Information to third parties such as Meta or Snapchat.

30. Because Defendant disclosed Plaintiff Santiago's Personal Viewing Information (including his FID, his phone number or email address, device identifiers, his purchase of a subscription, the title of the prerecorded video material he requested or obtained from Defendant's website as a paying subscriber, and the URL where such video is available to paying subscribers) to third parties during the applicable statutory period, Defendant violated Plaintiff Santiago's rights under the VPPA and invaded his statutorily conferred interest in keeping such information (which bears on his personal affairs and concerns) private.

IV. Plaintiff Smith

31. Plaintiff Smith is, and at all times relevant hereto was, a citizen and resident of Chattanooga, Tennessee.

32. Plaintiff Smith is, and at all times relevant hereto was, a user of Meta.

33. Plaintiff Smith is a consumer of the video products and services offered on Defendant's website and streaming service. Plaintiff Smith first subscribed to the MLB.com Website in April 2008. He subscribed to Defendant's MLB.tv streaming service in or about May

2023, and maintained his subscription until September 2023. Plaintiff Smith became a subscriber to Defendant's website and streaming service by registering for an account or paying for a subscription via Defendant's website, including by providing his name, email address, payment information, and zip code.

34. On multiple occasions during the two years preceding the filing of this action, Plaintiff Smith used his subscription to Defendant's website to request and obtain prerecorded videos from Defendant. On each such occasion, Defendant disclosed to Meta Plaintiff Smith's FID coupled with the specific title of the video he requested or obtained and the URL where he requested access to and obtained the video, among other information concerning Plaintiff Smith and the device on which he used to request and obtain the video.

35. On multiple occasions during the two years preceding the filing of this action, Plaintiff Smith used his subscription to Defendant's MLB.tv streaming service to request and obtain prerecorded videos from Defendant. On each such occasion, Defendant disclosed to Meta Plaintiff Smith's FID coupled with the specific title of the video he requested or obtained and the URL where he requested access to and obtained the video, among other information concerning Plaintiff Smith and the device on which he used to request and obtain the video.

36. At all times relevant hereto, including when obtaining a subscription to Defendant's website and purchasing a subscription to Defendant's streaming service, Plaintiff Smith had a Meta account, a Meta profile, and an FID associated with such profile.

37. Plaintiff Smith has never consented, agreed, authorized, or otherwise permitted Defendant to disclose his Personal Viewing Information to Meta. In fact, Defendant has never even provided Plaintiff Smith with written notice of its practices of disclosing its subscribers' Personal Viewing Information to third parties such as Meta.

38. Because Defendant disclosed Plaintiff Smith's Personal Viewing Information (including his FID, the title of the prerecorded video material he requested or obtained from Defendant's website as a paying subscriber, and the URL where such video is available to paying subscribers) to Meta during the applicable statutory period, Defendant violated Plaintiff Smith's rights under the VPPA and invaded his statutorily conferred interest in keeping such information (which bears on his personal affairs and concerns) private.

V. Defendant Major League Baseball Advanced Media L.P.

39. Defendant is a limited partnership that maintains its headquarters and principal place of business at 1271 Avenue of the Americas, New York, NY 10020.

40. Defendant operates and maintains the MLB.com Website and affiliate websites for each of the thirty Major League Baseball teams, where it offers consumers the opportunity to establish an ongoing relationship with Defendant via free subscription to *inter alia* access prerecorded video material and receive periodic notifications and updates on baseball content in exchange for the consumer providing detailed information about themselves and their device. Defendant also operates and maintains the streaming service MLB.tv, which allows consumers to become paid subscribers to access an expanded digital library of premium content, including documentaries, classic programs, interviews, World Series films, and more.

JURISDICTION AND VENUE

41. This Court has subject-matter jurisdiction over this civil action pursuant to 28 U.S.C. § 1331 and 18 U.S.C. § 2710.

42. Personal jurisdiction and venue are proper because Defendant maintains its headquarters and principal place of business in New York, NY, within this judicial District.

VIDEO PRIVACY PROTECTION ACT

43. Generally speaking, the VPPA prohibits companies like Defendant from knowingly disclosing to third parties like Facebook and Snapchat information that personally identifies consumers like Plaintiffs as having viewed particular videos or other audio-visual products or services.

44. Specifically, subject to certain exceptions that do not apply here, the VPPA prohibits "a video tape service provider" from "knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such provider[.]" 18 U.S.C. § 2710(b)(1). The statute defines a "video tape service provider" as "any person, engaged in the business…of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials," 18 U.S.C. § 2710(a)(4), and defines a "consumer" as "a renter, purchaser, or subscriber of goods or services from a video tape service provider." 18 U.S.C. § 2710(a)(1). "'[P]ersonally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3)

45. The VPPA's purpose is as apropos today as it was at the time of its enactment over 35 years ago. Leading up to the statute's enactment in 1988, members of the United States Senate warned that "[e]very day Americans are forced to provide to businesses and others personal information without having any control over where that information goes." *Id.* Senators at the time were particularly troubled by disclosures of records that reveal consumers' purchases and rentals of videos and other audiovisual materials, because such records offer "a window into our loves, likes, and dislikes," such that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and

pervasive form of surveillance." S. Rep. No. 100-599 at 7-8 (1988) (statements of Sens. Simon and Leahy, respectively).

46. Thus, in proposing the Video and Library Privacy Protection Act (which later became the VPPA), Senator Patrick J. Leahy (the senior Senator from Vermont from 1975 to 2023) sought to codify, as a matter of law, that "our right to privacy protects the choice of movies that we watch with our family in our own homes." 134 Cong. Rec. S5399 (May 10, 1988). As Senator Leahy explained at the time, it is the personal nature of such information, and the need to protect it from disclosure, that is the raison d'être of the statute: "These activities are at the core of any definition of personhood. They reveal our likes and dislikes, our interests and our whims. They say a great deal about our dreams and ambitions, our fears and our hopes. They reflect our individuality, and they describe us as people." *Id*.

47. While these statements rang true in 1988 when the act was passed, the importance of legislation like the VPPA in the modern era of data mining is more pronounced than ever before. During a recent Senate Judiciary Committee meeting, "The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century," Senator Leahy emphasized the point by stating: "While it is true that technology has changed over the years, we must stay faithful to our fundamental right to privacy and freedom. Today, social networking, video streaming, the 'cloud,' mobile apps and other new technologies have revolutionized the availability of Americans' information."[3]

[3] The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century, Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law, http://www.judiciary.senate.gov/meetings/the-video-privacy-protection-act-protecting-viewer-privacy-in-the-21stcentury.

48. Former Senator Al Franken may have said it best: "If someone wants to share what they watch, I want them to be able to do so . . . But I want to make sure that consumers have the right to easily control who finds out what they watch—and who doesn't. The Video Privacy Protection Act guarantees them that right."[4]

49. In this case, however, Defendant deprived Plaintiffs and the unnamed Class members of that right by systematically (and surreptitiously) disclosing their Personal Viewing Information to Facebook and Snapchat, without providing notice to (let alone obtaining consent from) any of them, as explained in detail below.

BACKGROUND FACTS

I. Consumers' Personal Information Has Real Market Value

50. In 2001, Federal Trade Commission ("FTC") Commissioner Orson Swindle remarked that "the digital revolution . . . has given an enormous capacity to the acts of collecting and transmitting and flowing of information, unlike anything we've ever seen in our lifetimes . . . [and] individuals are concerned about being defined by the existing data on themselves."[5]

51. More than a decade later, Commissioner Swindle's comments ring truer than ever, as consumer data feeds an information marketplace that supports a $26 billion dollar per year online advertising industry in the United States.[6]

---

[4] Chairman Franken Holds Hearing on Updated Video Privacy Law for 21st Century, frank.senate.gov (Jan. 31, 2012).

[5] FCC, *The Information Marketplace* (Mar. 13, 2001), at 8-11, *available at* https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

[6] *See Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html.

52. The FTC has also recognized that consumer data possesses inherent monetary value within the new information marketplace and publicly stated that:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[7]

53. In fact, an entire industry exists while companies known as data aggregators purchase, trade, and collect massive databases of information about consumers. Data aggregators then profit by selling this "extraordinarily intrusive" information in an open and largely unregulated market.[8]

54. The scope of data aggregators' knowledge about consumers is immense: "If you are an American adult, the odds are that [they] know[] things like your age, race, sex, weight, height, marital status, education level, politics, buying habits, household health worries, vacation dreams—and on and on."[9]

55. Further, "[a]s use of the Internet has grown, the data broker industry has already evolved to take advantage of the increasingly specific pieces of information about consumers that are now available."[10]

---

[7] Statement of FTC Cmr. Harbour (Dec. 7, 2009), at 2, *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

[8] *See* M. White, *Big Data Knows What You're Doing Right Now*, TIME.com (July 31, 2012), http://moneyland.time.com/2012/07/31/big-data-knows-what-youre-doing-right-now/.

[9] N. Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, N.Y. Times (June 16, 2012), *available at* http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of- consumer-database-marketing.html.

[10] Letter from Sen. J. Rockefeller IV, Sen. Cmtee. on Commerce, Science, and Transportation, to S. Howe, Chief Executive Officer, Acxiom (Oct. 9, 2012) *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=3bb94703-5ac8-4157-a97b-a658c3c3061c.

56. Recognizing the serious threat the data mining industry poses to consumers' privacy, on July 25, 2012, the co-Chairmen of the Congressional Bi-Partisan Privacy Caucus sent a letter to nine major data brokerage companies seeking information on how those companies collect, store, and sell their massive collections of consumer data, stating in pertinent part:

> By combining data from numerous offline and online sources, data brokers have developed hidden dossiers on every U.S. consumer. This large[-]scale aggregation of the personal information of hundreds of millions of American citizens raises a number of serious privacy concerns.[11]

57. Data aggregation is especially troublesome when consumer information is sold to direct-mail

58. Disclosures like Defendant's are particularly dangerous to the elderly. "Older Americans are perfect telemarketing customers, analysts say, because they are often at home, rely on delivery services, and are lonely for the companionship that telephone callers provide."[12] The FTC notes that "[t]she elderly often are the deliberate targets of fraudulent telemarketers who take advantage of the fact that many older people have cash reserves or other assets to spend on seemingly attractive offers."[13]

59. Indeed, an entire black market exists while the personal information of vulnerable elderly Americans is exchanged. Thus, information disclosures like Defendant's are particularly

---

[11] *See Bipartisan Group of Lawmakers Query Data Brokers About Practices Involving Consumers' Personal Information*, Website of Sen. Markey (July 24, 2012), http://www.markey.senate.gov/news/press-releases/bipartisan-group-of-lawmakers-query-data-brokers-about-practices-involving-consumers-personal-information.

[12] *Id.*

[13] *Fraud Against Seniors: Hearing before the Senate Special Committee on Aging* (August 10, 2000) (prepared statement of the FTC), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-fraud-against-seniors/agingtestimony.pdf.

troublesome because of their cascading nature: "Once marked as receptive to [a specific] type of spam, a consumer is often bombarded with similar fraudulent offers from a host of scam artists."[14]

60. Defendant is not alone in violating its subscribers' statutory rights and jeopardizing their well-being in exchange for increased revenue: disclosing customer and subscriber information to data aggregators, data appenders, data cooperatives, direct marketers, and other third parties has become a widespread practice. Unfortunately for consumers, however, this growth has come at the expense of their most basic privacy rights.

II. Consumers Place Monetary Value on their Privacy and Consider Privacy Practices When Making Purchases

61. As the data aggregation industry has grown, so too have consumer concerns regarding their personal information.

62. A recent survey conducted by Harris Interactive on behalf of TRUSTe, Inc. showed that 89 percent of consumers polled avoid doing business with companies who they believe do not protect their privacy online.[15] As a result, 81 percent of smartphone users polled said that they avoid using smartphone apps that they don't believe protect their privacy online.[16]

63. Thus, as consumer privacy concerns grow, consumers are increasingly incorporating privacy concerns and values into their purchasing decisions and companies viewed as having weaker privacy protections are forced to offer greater value elsewhere (through better quality and/or lower prices) than their privacy- protective competitors.

---

[14] *Id.*

[15] *See 2014 TRUSTe US Consumer Confidence Privacy Report*, TRUSTe, http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf.

[16] *Id.*

64. In fact, consumers' personal information has become such a valuable commodity that companies are beginning to offer individuals the opportunity to sell their personal information themselves.[17]

65. These companies' business models capitalize on a fundamental tenet underlying the personal information marketplace: consumers recognize the economic value of their private data. Research shows that consumers are willing to pay a premium to purchase services from companies that adhere to more stringent policies of protecting their personal data.[18]

66. Thus, in today's digital economy, individuals and businesses alike place a real, quantifiable value on consumer data and corresponding privacy rights.[19] As such, where a business offers customers a service that includes statutorily guaranteed privacy protections, yet fails to honor these guarantees, the customer receives a service of less value than the service paid for.

III. Defendant Uses Tracking Technology to Systematically Disclose its Customers' Personal Viewing Information to Third Parties

67. As alleged below, when a subscriber to Defendant's website ("Website subscriber") requests or obtains a specific video by clicking on the video on Defendant's website, the pixel technology that Defendant knowingly and intentionally installed on its website, transmits

[17] *See* Joshua Brustein, *Start-Ups Seek to Help Users Put a Price on Their Personal Data*, N.Y. Times (Feb. 12, 2012), *available at* http://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html.

[18] *See* Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (2011); *see also* European Network and Information Security Agency, *Study on monetising privacy* (Feb. 27, 2012), *available at* https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy.

[19] *See* Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Oct. 2003) at 2, *available at* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.321.6125&rep=rep1&type=pdf ("It is obvious that people value online privacy.").

the subscriber's personally identifying information and detailed information concerning the specific interactions the Website subscriber takes on its website (including the subscriber's Personal Viewing Information revealing the specific videos that he or she requested) to Meta and Snapchat, without the Website subscriber's consent and in clear violation of the VPPA.

68. Also, when a subscriber to Defendant's streaming service ("Streaming Service subscriber") purchases a subscription and later requests or obtains a specific video by clicking on the video on Defendant's website, the pixel technology that Defendant knowingly and intentionally installed on its website, transmits the subscriber's personally identifying information and detailed information concerning the specific interactions the Streaming Service subscriber takes on its website (including the subscriber's Personal Viewing Information revealing that a subscription was purchased and that specific videos were requested or obtained) to Meta and Snapchat, without the Streaming Service subscriber's consent and in clear violation of the VPPA.

A. The Meta Pixel

69. On February 4, 2004, Mark Zuckerberg and others launched Facebook, now known as "Meta".[20] Since then, Meta has become the world's largest social media platform. To create a Meta account, a person must provide, *inter alia*, his or her first and last name, birthdate, gender, and phone number or email.

70. The Meta Pixel, first introduced in 2013 as the "Facebook Pixel," is a unique string of code that companies can embed on their websites to allow them to track consumers' actions and report the actions back to Meta.

71. The Meta Pixel allows online-based companies like Defendant to build detailed

[20] Meta, *Company Info*, https://about.fb.com/company-info./.

profiles about their visitors by collecting information about how they interact with their websites, and to then use the collected information to service highly targeted advertising to them.

72. Additionally, a Meta Pixel installed on a company's website allows Meta "to match . . . website visitors to their respective [Meta] User accounts."[21] Meta is able to do this because it has assigned to each of its users an "FID" number – a unique and persistent identifier that allows anyone to look up the user's unique Meta profile and thus identify the user by name[22] – and because each transmission of information made from a company's website to Meta via the Meta Pixel is accompanied by, *inter alia*, the FID of the website's visitor.

73. The FID is stored in a small piece of code known as a "cookie" that Meta launches and stores in the internet browsers of each Meta accountholder's device(s) to distinguish between website visitors.[23]

74. As Meta's developer's guide explains, installing the Meta Pixel on a website allows Meta to track actions that users with Meta accounts take on the site. Meta states that "Examples of [these] actions include adding an item to their shopping cart or making a purchase."[24]

---

[21] Meta, *Get Started—Meta Pixel*, https://developers.facebook.com/docs/meta-pixel/get-started/

[22] For example, Mark Zuckerberg's FID is reportedly the number "4," so logging into Facebook and typing www.facebook.com/4 in the web browser retrieves Mark Zuckerberg's Facebook page: www.facebook.com/zuck, and all of the additional personally identifiable information contained therein.

[23] Meta, *How to Create a Custom Audience from Your Customer List*, https://www.facebook.com/business/help/471978536642445?id=1205376682832142 (last visited Nov. 11, 2024).

[24] Meta, *About Meta Pixel*, available at https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

75. The default configuration of the Meta Pixel, which is what Defendant used, enables website visitor tracking because the Meta Pixel automatically detects first-party cookie data from the particular website that the visitor is on and then automatically matches it with third-party cookie data from Meta such as the c_user cookie that houses a person's FID.[25]

76. Meta's Business Tools Terms govern the use of Meta's Business Tools, including the Meta Pixel.[26]

77. Meta's Business Tools Terms state that website operators may use Meta's Business Tools, including the Meta Pixel, to transmit the "Contact Information" and "Event Data" of their website visitors to Meta.

78. Meta's Business Tools Terms define "Contact Information" as "information that personally identifies individuals, such as names, email addresses, and phone numbers . . . ."[27]

79. Meta's Business Tools Terms state: "You instruct us to process the Contact Information solely to match the Contact Information against user IDs [e.g., FIDs] ("Matched User IDs"), as well as to combine those user IDs with corresponding Event Data."[28]

---

[25] Meta, *Business Help Center: About cookie settings for the Meta Pixel*, FACEBOOK, https://www.facebook.com/business/help/471978536642445?id=2105376682832142 (last visited Nov. 11, 2024).

[26] Meta, *Meta Business Tools Terms*, available at https://www.facebook.com/legal/technology_terms.

[27] *Id.*

[28] *Id.*

80. The Business Tools Terms define "Event Data" as, *inter alia*, "information that you share about people and the actions that they take on your websites and apps or in your shops, such as visits to your sites, installations of your apps, and purchases of your products."[29]

81. Website operators use the Meta Pixel to send information about visitors to their websites to Meta. Every transmission to Meta accomplished through the Meta Pixel includes at least two elements: (1) the website visitor's FID and (2) the webpage's URL triggering the transmission.

82. Depending on the configuration of the Meta Pixel, the website may also send Event Data to Meta. Defendant has configured the Meta Pixel on its website and streaming service to send Event Data to Meta, including the page view and purchase events.

83. When website operators make transmissions to Meta through the Meta Pixel, none of the following categories of information are hashed or encrypted: the visitor's FID, the website URL, or the Event Data.

84. Every website operator installing the Meta Pixel must agree to the Meta Business Tools Terms.[30]

85. Moreover, the Meta Pixel can follow a consumer to different websites and across the Internet even after clearing browser history.

86. Meta has used the Meta Pixel to amass a vast digital database of dossiers comprised of highly detailed personally identifying information about each of its billions of users worldwide, including information about all of its users' interactions with any of the millions of websites across

[29] *Id*.

[30] *See id*.

the Internet on which the Meta Pixel is installed. Meta then monetizes this Orwellian database by selling advertisers the ability to serve highly targeted advertisements to the persons whose personal information is contained within it.

87. Simply put: if a company chooses to install the Meta Pixel on its website, both the company who installed it and Meta (the recipient of the information it transmits) are then able to "track[] the people and type of actions they take"[31] on the company's website, including the purchases they made, the items they spent time viewing, and, as relevant here, the specific video content that they requested or obtained on the website, the purchase of a subscription to access prerecorded video content, and the specific video content that they requested or obtained from the streaming service.

B. Defendant Knowingly Uses the Meta Pixel to Transmit the Personal Viewing Information of its Subscribers to Meta

88. Defendant allows persons to become digital consumers of its various online-based video products and services by subscribing to its website and or streaming service.

89. To subscribe to Defendant's website, the consumer must provide his or her email address, date of birth, and indicate whether or not he or she will consent to receive commercial e-mails from Defendant and their partners.

90. When subscribing to Defendant's website, the consumer unknowingly provides his or her name, device identifiers, IP address, browser information, and FID because Defendant programmed the Meta Pixel to automatically collect this information from the cookies on the consumer's device and disclose this information to Meta.

91. To subscribe to Defendant's streaming service, the consumer must provide at least

[31] Meta, *Retargeting: How to Advertise to Existing Customers with Ads on Facebook*, https://www.facebook.com/business/goals/retargeting.

his or her name, email address, billing address, and credit- or debit-card (or other form of payment) information.

92. After a person has completed the subscription process for the streaming service and gains access to videos on Defendant's website, Defendant uses – and has used at all times relevant hereto – the Meta Pixel to disclose to Meta the unencrypted FID of the subscriber and the specific videos that he or she requested or obtained from Defendant's website.

93. Defendant intentionally programmed its website and streaming service (by following step-by-step instructions from Meta's website) to include a Meta Pixel that systematically transmits to Meta the FIDs of its Streaming Service subscribers, the purchase of a subscription, and the video products that each of them requested in order to take advantage of the targeted advertising and other informational and analytical services offered by Meta.

94. With only a person's FID and the subscription or video content name or URL that the person requested on Defendant's website—all of which Defendant knowingly provides to Meta —any ordinary person could learn the identity of the person to whom the FID corresponds and the specific video products or services that this person requested. This can be accomplished simply by accessing the URL www.facebook.com/[unencrypted FID/].

95. Defendant's practices of disclosing the Personal Viewing Information of its subscribers to Meta continued unabated for the full duration of the time period relevant to this action. At all times relevant hereto, whenever Plaintiffs or another Website or Streaming Service subscriber requested a particular video (by clicking on it) on Defendant's website, Defendant disclosed to Meta that (*inter alia*) the specific video that was requested (including the URL where such video was accessed), along with the FID of the Website or Streaming Service subscriber who requested it (which, as discussed above, uniquely identifies the person).

96. At all relevant times, Defendant knew that the Meta Pixel disclosed its subscribers' Personal Viewing Information to Meta.

97. Defendant could easily have programmed its website and streaming service so that none of its subscribers' detailed Personal Viewing Information is disclosed to Meta. Instead, Defendant chose to program its website and streaming service so that all of its subscribers' detailed Personal Viewing Information is sent to Meta *en masse*.

98. Prior to transmitting its subscribers' Personal Viewing Information to Meta, Defendant failed to notify Plaintiffs or any of its other subscribers that it would do so, and neither Plaintiffs nor any of its other subscribers have consented (in writing or otherwise) to these practices.

99. By intentionally disclosing to Meta Plaintiffs' and its other subscribers' FIDs together with the specific video content they each requested or obtained, without Plaintiffs' or any of its other subscribers' consent to these practices, Defendant knowingly and systematically violated the VPPA on an enormous scale.

C. The Snapchat Pixel

100. In September 2011, Snapchat launched Picaboo which later transformed into what is now known as "Snapchat." Snapchat is an app offering an easy and fast way "way to communicate the full range of human emotions with your friends without pressure to be popular, pretty, or perfect."[32] To create a Snapchat account, a person must provide, *inter alia*, his or her first and last name, birth date (user must be over 13 years old), gender, and cellular telephone

[32] Snap Inc. Investor Relations, *About Snap*, https://investor.snap.com/about-snap/default.aspx (last visited Nov. 20, 2024).

number or email address.[33]

101. The Snapchat Pixel, first introduced in 2017, is a unique piece of code that can be placed on websites to share website events with Snapchat to measure the cross-device impact of ad campaigns and to optimize ad campaigns for driving leads, finding new customers or subscribers, and increasing product sales. This allows companies like Defendant to build detailed profiles about their customers and to serve them with highly targeted advertising.

102. Websites like Defendant's can transmit through the Snapchat Pixel the following information: device platform, webpage URLs viewed, session ID, anonymous user ID, browser information, event codes, currency, email addresses, and phone numbers.

103. Additionally, the Snapchat Pixel installed on a company's website allows the company to pass through or share its customers' Contact Details – name, email address, and or phone number – with Snapchat, for manual and automated matching purposes.[34] This is because Snapchat collects Contact Information when a person first registers for a Snapchat account – such as first and last name and phone number – which Snapchat then uses to assign a unique and persistent identifier. The Snapchat identifier does not prevent Snapchat or anyone else from discovering a person's name by simply looking it up based on their phone number or email address, however. The phone number is still connected to the Snapchat account, and the transmissions made from a company's website to Snapchat via the Snapchat Pixel during the user's continuous session are accompanied by, *inter alia*, the phone number or email address of

---

[33] Snapchat Help Center, *How to Create a Snapchat Account*, https://help.snapchat.com/hc/en-us/articles/7012333136788-How-to-Create-a-Snapchat-Account (last visited Nov. 20, 2024).

[34] Snapchat Business Help, *Getting Started with Enabling the Pixel*, https://businesshelp.snapchat.com/s/article/pixel-website-install?language=en_US (last visited Nov. 20, 2024).

the website's visitor. Moreover, the Snapchat Pixel can and does follow a consumer to different websites and across the Internet even after the consumer's browser history has been cleared.

104. Snapchat has used the Snapchat Pixel to amass a vast digital database of dossiers comprised of highly detailed personally identifying information about each of its millions of users worldwide, including information about all its users' interactions with any of the hundreds of thousands of websites across the Internet on which the Snapchat Pixel is installed. Snapchat then monetizes its database by selling advertisers the ability to serve highly targeted advertisements to the persons whose personal information is contained within it.

105. Simply put, if a company chooses to install the Snapchat Pixel on its website, both the company who installed it and Snapchat (the recipient of the information it transmits) are then able to track the user's interactions with that particular webpage including, as relevant here, the subscription to access prerecorded video material purchased or the specific prerecorded video material that is watched, and thus is requested or obtained on Defendant's website or streaming service.

D. Defendant Knowingly Uses the Snapchat Pixel to Transmit the Personal Viewing Information of its Customers to Snapchat

106. Similar to the Meta Pixel, during the purchase or registration process and each subsequent session on Defendant's Website or streaming service, Defendant uses – and has used at all times relevant hereto – the Snapchat Pixel to disclose to Snapchat the device platform, webpage URLs viewed, session ID, anonymous user ID, browser information, event codes, currency, and phone number of the person who made the purchase and the subscription title or specific title of video material that the person requested or obtained (as well as the URL where such video material is available).

107. In order to take advantage of the targeted advertising and other informational and

analytical services offered by Snapchat, Defendant intentionally programmed its Website and Streaming Service (by following step-by-step instructions from Snapchat's website) to include the Snapchat Pixel code, which systematically transmits to Snapchat personally identifiable information (a person's cell phone number, email address, and other unique device information) of each person with a Snapchat account who requests or obtains prerecorded video material as a subscriber of Defendant's Website or Streaming Service, along with information revealing whether a subscription was purchased to access prerecorded video material and the specific titles of prerecorded video content that the person requested or obtained.

108. Snapchat automatically matches off-Snapchat users across devices to their Snapchat accounts by using a first-party cookie, a small piece of code, that Snapchat launches and stores in the internet browsers of each Snapchat accountholder's device(s) to distinguish between website visitors and that cookie value is captured by the Snapchat Pixel when actions are taken on a particular website.[35] The Snapchat first-party cookie used to identify users is the "sc_at" cookie,[36] which stores a unique variable (combination of letters, numbers, and characters) that Snapchat assigns to each Snapchat user on their website.

109. With Defendant's configuration of the Snapchat Pixel, Defendant discloses its subscribers' email addresses and phone numbers to Snapchat and the subscription purchase information or specific title of prerecorded video content watched on its Website or Streaming Service along with all Snapchat account information stored in the "sc_at" cookie as made clear by

---

[35] Snapchat Business Help, *Getting Started with Enabling the Pixel*, https://businesshelp.snapchat.com/s/article/pixel-website-install?language=en_US (last visited Nov. 20, 2024).

[36] Snap Inc., *Cookie Information*, https://www.snap.com/privacy/cookie-information?lang=en-US#preferences (last visited Nov. 20, 2024).

Defendant's use of its own first-party cookie that has the exact same value of the "sc_at" cookie uniquely known and assigned by Snapchat.

110. With only a person's cell phone number or email address and the subscription purchase information or the title of the prerecorded video material (or URL where such material is available for purchase) that the person requested or obtained from Defendant's website or streaming service—all of which Defendant knowingly and systematically provides to Snapchat—Snapchat is able to "automatically match" an off-Snapchat user with his or her Snapchat account with that person's registered name, just like any ordinary person could learn the identity of the person to whom the cell phone number or email address corresponds by simply, among other ways, doing a free online reverse lookup. Once looked up, that ordinary person has discovered a person's identity and the subscription or the title of the specific prerecorded video material that the person purchased (and thus requested and obtained).

111. Defendant's practice of disclosing the Personal Viewing Information of its subscribers to Snapchat continued unabated for the duration of the two-year period preceding the filing of this action. At all times relevant hereto, whenever Plaintiffs or any other person purchased a subscription to access prerecorded video material or requested or obtained prerecorded video material from Defendant, Defendant disclosed to Snapchat (*inter alia*) the subscription or the specific title of the video material requested or obtained (including the URL where such material is available for purchase), along with the Snapchat persistent identifier of the person who purchased or watched it (which, as discussed above, uniquely identified the person).

112. At all times relevant hereto, Defendant knew the Snapchat Pixel was disclosing its subscribers' Personal Viewing Information to Snapchat.

113. Although Defendant could easily have programmed its website so that none of its

subscribers' Personal Viewing Information is disclosed to Snapchat, Defendant instead chose to program its Website and Streaming Service so that all of its customers' Personal Viewing Information is disclosed to Snapchat.

114. Before transmitting its subscribers' Personal Viewing Information to Snapchat, Defendant failed to notify any of them that it would do so, and none of them have ever consented (in writing or otherwise) to these practices.

115. By intentionally disclosing to Snapchat Plaintiffs' and its other subscribers' phone numbers or email addresses together with subscription purchase information or the specific video material that they each requested or obtained, without any of their consent to these practices, Defendant knowingly violated the VPPA on an enormous scale.

CLASS ACTION ALLEGATIONS

116. There are three classes that have been injured by Defendant's use of tracking technologies, which are:

a. **Streaming Service Class – Meta**: Plaintiffs collectively seek to represent a class defined as all persons in the United States who, during the two years preceding the filing of this action, requested or obtained video content from Defendant's streaming service as a subscriber and while maintaining an account with Meta Platforms, Inc. f/k/a Facebook, Inc.

b. **Website Viewing Class – Meta**[37]: Plaintiff Smith seeks to represent a class defined as all persons in the United States who, during the two years preceding the filing of this action, requested or obtained video content from Defendant's website or affiliate websites as a subscriber of Defendant's website and while maintaining an account with Meta Platforms, Inc. f/k/a Facebook, Inc.

c. **Snapchat Pixel Class**: Plaintiff Santiago seeks to represent a class defined as all persons in the United States who, during the two years preceding the filing of this action, requested or obtained video content from Defendant's streaming service as a subscriber or requested or obtained video content from Defendant's website or affiliate websites as a subscriber thereto and while maintaining an account with Snapchat.

[37] The Streaming Service Class and Website Viewing Class are collectively referred to herein as the "Meta Classes."

117. Members of the Classes are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Classes number in at least the tens of thousands. The precise number of members for each Class and their identities are unknown to Plaintiffs at this time but may be determined through discovery. Members of the Classes may be notified of the pendency of this action by mail and/or publication through the membership records of Defendant.

118. Common questions of law and fact exist for all members of the Classes and predominate over questions affecting only individual class members. Common legal and factual questions include, but are not limited to: (a) whether Defendant knowingly disclosed Plaintiffs' and Class members' Personal Viewing Information to third parties; (b) whether Defendant's conduct violates the Video Privacy Protection Act, 18 U.S.C. § 2710; (c) whether Defendant should be enjoined from disclosing Plaintiffs' and members of the Classes' Personal Viewing Information to third parties; and (d) whether Plaintiffs and Class members are entitled to statutory damages for the aforementioned violations.

119. The named Plaintiffs' claims are typical of the claims of the Classes in that the named Plaintiffs and members of the Classes suffered invasions of their statutorily protected right to privacy (as afforded by the VPPA), as well as intrusions upon their private affairs and concerns that would be highly offensive to a reasonable person, as a result of Defendant's uniform and wrongful conduct in intentionally disclosing their Personal Viewing Information to third parties.

120. Plaintiffs are adequate representatives of the Classes because their interests do not conflict with the interests of the members of the Classes that they seek to represent, they have retained competent counsel experienced in prosecuting class actions, and they intend to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the interests

of members of the Classes.

121. The class mechanism is superior to other available means for the fair and efficient adjudication of the Classes' claims. Each individual Class Member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by this case's complex legal and factual issues. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

CAUSE OF ACTION
(Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710)

122. Plaintiffs repeat the allegations asserted in the preceding paragraphs as if fully set forth herein.

123. Plaintiffs bring their claims individually and on behalf of the putative Class Members against Defendant.

124. The VPPA prohibits a "video tape service provider" from knowingly disclosing "personally identifying information" concerning any "consumer" to a third-party without the "informed, written consent (including through an electronic means using the Internet) of the consumer." 18 U.S.C. § 2710.

125. As defined in 18 U.S.C. § 2710(a)(4), a "video tape service provider" is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or

delivery of prerecorded video cassette tapes or similar audiovisual materials[.]" Defendant is a "video tape service provider" as defined in 18 U.S.C. § 2710(a)(4) because it is engaged in the business of renting, selling, or delivering audiovisual materials that are similar to prerecorded video cassette tapes through its MLB.com Website and affiliate team sites and through its MLB.tv Streaming Service, and those rentals, sales, or deliveries affect interstate or foreign commerce.

126. As defined in 18 U.S.C. § 2710(a)(1), a "'consumer' means any renter, purchaser, or consumer of goods or services from a video tape service provider." Plaintiffs and Streaming Service Class members, as subscribers of Defendant's MLB.tv Streaming Service that provides them prerecorded video content, are "consumers" as defined in 18 U.S.C. § 2710(a)(1). Plaintiff Smith and Website Viewing Class members, as subscribers of Defendant's MLB.com Website that provides prerecorded video content, are consumers as defined in 18 U.S.C. § 2710(a)(1). Plaintiff Santiago and Snapchat Pixel Class members, as subscribers of Defendant's MLB.tv Streaming Service and Defendant's MLB.com Website providing prerecorded video content, are consumers as defined in 18 U.S.C. § 2710(a)(1).

127. As defined in 18 U.S.C. § 2710(a)(3), "'personally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." The Personal Viewing Information that Defendant transmitted to Meta and Snapchat constitutes personally identifiable information as defined in 18 U.S.C. § 2710(a)(3) because it identified each of the Plaintiffs and members of the Classes to third parties as an individual who purchased, and thus "requested or obtained," a subscription to access prerecorded video material or who watched, and thus "requested or obtained," specific prerecorded video material from Defendant's website or streaming service in the manner alleged herein.

128. Defendant never obtained informed, written consent from Plaintiffs or any Class member to disclose their Personal Viewing Information to Meta, Snapchat, or any other third party. More specifically, Defendant never obtained from Plaintiffs or any member of the Classes informed, written consent in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer; Defendant never obtained from Plaintiffs or any member of the Classes informed, written consent that, at the election of the consumer, was given at the time the disclosure is sought or was given in advance for a set period of time, not to exceed two years or until consent is withdrawn by the consumer, whichever is sooner; and Defendant never provided an opportunity, in a clear and conspicuous manner, for Plaintiffs or any member of the Classes to withdraw consent on a case-by-case basis or to withdraw consent from ongoing disclosures, at the consumer's election. *See* 18 U.S.C. § 2710(b)(2).

129. Defendant knowingly disclosed Plaintiffs' and members of the Meta Classes' Personal Viewing Information to Meta via the Meta Pixel technology because Defendant intentionally installed and programmed the Meta Pixel code on its website and streaming service, knowing that such code would transmit the title of the subscription purchased or prerecorded video material watched by its subscribers and each subscriber's unique identifiers (including FIDs).

130. Defendant knowingly disclosed Plaintiff Santiago and Snapchat Pixel Class Members' Personal Viewing Information to Snapchat via the Snapchat Pixel technology because Defendant intentionally installed and programmed the Snapchat Pixel code on its Website and streaming service, knowing that such code would transmit the subscription purchased or prerecorded video material watched by its subscribers and the subscribers' cellular telephone number or email address, browser, and device information.

131. By disclosing Plaintiffs' and members of the Classes' Personal Viewing

Information, Defendant violated their statutorily protected right to privacy in the videos they requested or obtained from Defendant. 18 U.S.C. § 2710(c).

132. As a result of these violations, Defendant is liable to Plaintiffs and members of the Classes for damages and other relief as provided by the VPPA.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek a judgment against Defendant Major League Baseball Advanced Media L.P. as follows:

A. For an order certifying the Classes under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiffs as representatives of the Classes and Plaintiffs' attorneys as Class Counsel to represent the Classes;

B. For an order declaring that Defendant's conduct as described herein violated the VPPA;

C. For an order finding in favor of Plaintiffs and the Classes and against Defendant on all counts asserted herein;

D. For an award of $2,500.00 to the Plaintiffs and each member of the Classes, as provided by the VPPA, 18 U.S.C. § 2710(c);

E. For an order permanently enjoining Defendant from disclosing the Personal Viewing Information of its Website and Streaming Service subscribers to third parties in violation of the VPPA.

F. For prejudgment interest on all amounts awarded; and

G. For an order awarding punitive damages, reasonable attorneys' fees, and costs to counsel for Plaintiffs and the Class under Rule 23 and 18 U.S.C. § 2710(c).

DEMAND FOR TRIAL BY JURY

Plaintiffs demand a trial by jury on all causes of action and issues so triable.

Dated: November 22, 2024

Respectfully submitted,

HEDIN LLP

/s/Elliot O. Jackson
ELLIOT O. JACKSON
NEW YORK REG. NO. 6076798
1395 BRICKELL AVE., SUITE 610
MIAMI, FLORIDA 33131-3302
TELEPHONE: (305) 357-2107
FACSIMILE: (305) 200-8801
EJACKSON@HEDINLLP.COM

Frank S. Hedin*
HEDIN LLP
1395 BRICKELL AVE., SUITE 610
MIAMI, FLORIDA 33131-3302
TELEPHONE: (305) 357-2107
FACSIMILE: (305) 200-8801
FHEDIN@HEDINLLP.COM

Attorneys for Plaintiffs and the Putative Class

* Pro Hac Vice Application forthcoming